HYBRID CRYPTOGRAPHIC ACCELERATOR AND METHOD OF OPERATION THEREOF

ABSTRACT OF THE DISCLOSURE

For use in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, a cryptographic accelerator, a method of performing cryptography therewith and an SoC incorporating the cryptographic accelerator or the method. In one embodiment, the cryptographic accelerator includes: (1) a key register located within the SEE and coupled to the secure memory to receive a cryptographic key therefrom and (2) data input and output registers located outside of the SEE and coupled to the key register to allow the cryptographic key to be applied to input data arriving via the data input register to yield output data via the data output register.